(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2016 년 9 월 22 일 (22.09.2016)

WIPO | PCT

(10) 국제공개번호
WO 2016/148471 A1

(51) 국제특허분류:
G06F 21/51 (2013.01) *G06F 21/52* (2013.01)
G06F 21/50 (2013.01)

(21) 국제출원번호: PCT/KR2016/002535

(22) 국제출원일: 2016 년 3 월 14 일 (14.03.2016)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2015-0035177 2015 년 3 월 13 일 (13.03.2015) KR
10-2016-0030568 2016 년 3 월 14 일 (14.03.2016) KR

(71) 출원인: 주식회사 에버스핀 (EVERSPIN CORP.) [KR/KR]; 08504 서울시 금천구 서부샛길 606, 비동 11 층 1110 호(가산동), Seoul (KR).

(72) 발명자; 겸
(71) 출원인 : 하영빈 (HA, Young Bin) [KR/KR]; 07360 서울시 영등포구 여의대방로 43 나길 25, 101 동 608 호 (신길동, 삼환아파트), Seoul (KR).

(74) 대리인: 강태훈 (KANG, Tae Hoon) 등; 06731 서울시 서초구 서운로 26-1, 701 호 (서초동, 보일빌딩 7 층), Seoul (KR).

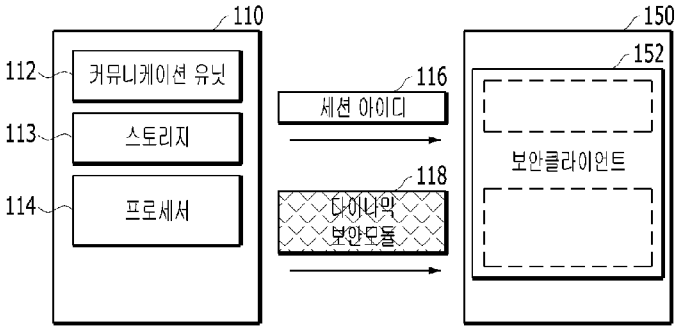
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:
— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) Title: DYNAMIC SECURITY MODULE SERVER DEVICE AND OPERATING METHOD THEREOF

(54) 발명의 명칭 : 다이나믹 보안모듈 서버장치 및 그 구동방법



112 ... Communication unit
113 ... Storage
114 ··· Processor
116 ··· Session ID
118 ··· Dynamic security module
152 ··· Security client

(57) Abstract: The present invention relates to a dynamic security module server device and an operating method thereof. The present invention transmits and receives a security management event from a user terminal and transmits a dynamic security module to a security client of the user terminal, wherein a portion or the entirety of a code which performs security management in the security client of the user terminal in which a security session has been generated is allowed to have an effective time.

(57) 요약서: 본 발명은 다이나믹 보안모듈 서버장치 및 그 구동방법에 관한 것으로, 사용자 단말로부터 보안관리 이벤트를 송수신하고, 다이나믹 보안모듈을 사용자 단말의 보안 클라이언트로 전송하되, 보안 세션이 생성된 사용자 단말의 보안 클라이언트에서 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 한다.

WO 2016/148471 A1

명세서

발명의 명칭: 다이나믹 보안모듈 서버장치 및 그 구동방법

기술분야

[1] 본 발명은 다이나믹 보안모듈 서버장치 및 그 구동방법에 관한 것으로, 더욱 상세하게는 보안관리를 수행하는 코드의 일부 또는 전부가 일정한 유효시간을 가지는 다이나믹 보안모듈을 사용자 단말의 보안 클라이언트로 전송하여, 사용자 단말의 각종 응용 프로그램들에 대한 보안모듈이 수시로 변경되도록 함으로써, 상기 응용 프로그램들에 대한 해킹이 어려워지도록 하여 사용자 단말의 보안성(security)을 현저하게 향상시킬 수 있는 다이나믹 보안모듈 서버장치 및 그 구동방법에 관한 것이다.

배경기술

[2] 최근, 모바일 단말인 스마트폰은 현대 생활에 없어서는 안될 필수품으로 자리잡았으며 전 세계적으로 널리 보급되고 있다. 그러나, 스마트폰의 보안 취약성이 계속적으로 발견되면서 악성 어플리케이션을 통한 공격이 급증하고 있다.

[3] 해커들은 모바일 단말을 대상으로 악성 어플리케이션을 개발하여 악성코드를 삽입한 후 이를 일반 사용자에게 오픈 마켓 또는 인터넷을 통해 정상 어플리케이션인 것처럼 위장해 배포한다. 악성 어플리케이션이 모바일 단말에 저장된 경우에, 모바일 단말 내의 악성 어플리케이션은 사용자도 모르게 SMS 송수신 정보, 전화번호부, 인터넷 접속 기록 등의 개인정보뿐만 아니라 모바일 뱅킹 등에 사용되는 모바일 공인인증서 등의 금융정보를 외부서버로 유출시키는 공격을 시도할 수 있다.

[4] 대부분의 어플리케이션 보안 솔루션은 어플리케이션이 실행되면 어플리케이션의 보안모듈과 통신하여 보안 로직을 호출하고 결과를 응답한다. 그러나, 해커들의 공격으로 보안 모듈과의 통신이 강제적으로 차단되거나 변조된 어플리케이션으로 인해 보안모듈이 무력화 된다면, 개인신상정보 및 금융과 관련된 개인정보에 치명적인 취약점이 발생하게 된다.

[5] 따라서, 최근 국내외적으로 널리 보급되고 있는 모바일 단말 기반 사용자 환경에서 보안 취약 문제를 해결하고, 사용자 단말에 포함된 다양한 소프트웨어의 보안성을 향상시킬 수 있는 기술개발에 대한 필요성이 크게 대두되고 있다.

발명의 상세한 설명

기술적 과제

[6] 본 발명의 목적은 상기와 같은 종래 기술의 문제점을 해결하고자 도출된 것으로서, 보안관리를 수행하는 코드의 일부 또는 전부가 일정한 유효시간을 가지는 다이나믹 보안모듈을 사용자 단말의 보안 클라이언트로 전송하여,

사용자 단말의 각종 응용 프로그램들에 대한 보안모듈이 수시로 변경되도록 함으로써, 상기 응용 프로그램들에 대한 해킹이 어려워지도록 하여 사용자 단말의 보안성(security)을 현저하게 향상시킬 수 있는 다이나믹 보안모듈 서버장치 및 그 구동방법에 관한 것이다.

과제 해결 수단

[7] 이러한 목적을 달성하기 위하여 본 발명에 따른 다이나믹 보안모듈 서버장치는 사용자 단말에 다이나믹 보안모듈을 전송하며, 사용자 단말로부터 보안관리 이벤트를 수신하는 다이나믹 보안모듈 서버장치로서, 네트워크를 통해 상기 보안관리 이벤트를 송수신 하는 커뮤니케이션 유닛 및 상기 커뮤니케이션 유닛을 제어하는 프로세서를 포함하고, 상기 프로세서는 상기 사용자 단말의 보안 클라이언트와 보안 세션을 생성하고, 상기 다이나믹 보안모듈을 상기 사용자 단말의 보안 클라이언트로 전송하되, 상기 보안 세션이 생성된 상기 사용자 단말의 보안 클라이언트에서 상기 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 하는 것으로 구성된다.

[8] 상기 프로세서는 상기 보안 클라이언트로 전송된 다이나믹 보안모듈로부터 보안관리 결과를 수신하고, 상기 수신한 보안관리 결과를 확인하여, 보안관리 확인 결과값을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 것을 더 포함할 수 있다.

[9] 상기 프로세서는 상기 사용자 단말에 보안문제 발생 시, 상기 사용자 단말의 응용 프로그램을 정지시키도록 하는 정지명령을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 것을 더 포함할 수 있다.

[10] 상기 프로세서는 보안 세션 식별자로서 세션 아이디를 생성하여 저장하고, 상기 세션 아이디를 상기 보안 클라이언트에 전송하여 상기 보안 클라이언트가 상기 세션 아이디를 저장하도록 하여, 상기 보안 세션을 생성할 수 있다.

[11] 상기 보안 세션의 생성은 인증이 완료된 사용자 단말의 보안 클라이언트와 생성할 수 있다.

[12] 상기 유효시간은 상기 유효시간의 경과 시 상기 코드의 일부 또는 전부가 삭제되거나, 사용되지 않도록 하는 유효시간일 수 있다.

[13] 상기 프로세서는 상기 보안 세션이 유지되는 동안 상기 보안 클라이언트로 전송된 각각의 상기 다이나믹 보안모듈에 대한 파라미터를 저장되도록 하는 것을 더 포함할 수 있다.

[14] 상기 프로세서는 상기 보안 클라이언트로부터 전송된 내역이 상기 다이나믹 보안모듈의 파라미터의 구성과 동일한 지를 검증하는 것을 더 포함할 수 있다.

[15] 상기 다이나믹 보안모듈 서버장치는 상기 사용자 단말의 보안 클라이언트로 전송할 다이나믹 보안모듈, 보안 세션 식별자로서 세션 아이디, 및 다이나믹 보안모듈에 대한 파라미터를 저장하는 스토리지를 더 포함할 수 있다.

[16] 상기 프로세서는 상기 다이나믹 보안모듈이 정상 동작했음을 증명하는

검증토큰을 상기 사용자 단말의 응용 프로그램 운용서버로 전송하는 것을 더 포함할 수 있다.

[17] 본 발명은 또한, 상기 목적을 달성하기 위하여, 사용자 단말에 다이나믹 보안모듈을 전송하며, 사용자 단말로부터 보안관리 이벤트를 수신하는 다이나믹 보안모듈 서버장치의 구동방법으로서, 상기 사용자 단말의 보안 클라이언트와 보안 세션을 생성하는 단계 및 상기 다이나믹 보안모듈을 상기 보안 세션이 생성된 상기 사용자 단말의 보안 클라이언트에서 상기 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 상기 사용자 단말의 보안 클라이언트로 전송하는 단계를 포함하는 다이나믹 보안모듈 서버장치의 구동방법을 제공한다.

[18] 상기 구동방법은 상기 보안 클라이언트로 전송된 다이나믹 보안모듈로부터 보안관리 결과를 수신하고, 상기 수신한 보안관리 결과를 확인하여, 보안관리 확인 결과값을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계를 더 포함할 수 있다.

[19] 상기 구동방법은 상기 사용자 단말에 보안문제가 발생 시, 상기 사용자 단말의 응용 프로그램을 정지시키도록 하는 정지명령을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계를 더 포함할 수 있다.

[20] 상기 구동방법은 보안 세션 식별자로서 세션 아이디를 생성하여 저장하고, 상기 세션 아이디를 상기 보안 클라이언트에 전송하여 상기 보안 클라이언트가 상기 세션 아이디를 저장하도록 하여, 상기 보안 세션을 생성할 수 있다.

[21] 상기 구동방법은 상기 보안 세션이 유지되는 동안 상기 보안 클라이언트로 전송된 각각의 상기 다이나믹 보안모듈에 대한 파라미터를 저장하는 단계를 더 포함할 수 있다.

[22] 본 발명은 또한, 상기 다이나믹 보안모듈 서버장치의 구동방법을 실행하기 위한 프로그램이 기록되어 있는 컴퓨터에서 판독 가능한 기록 매체를 제공한다.

발명의 효과

[23] 본 발명에 따른 다이나믹 보안모듈 서버장치 및 그 구동방법은 보안관리를 수행하는 코드의 일부 또는 전부가 일정한 유효시간을 가지는 다이나믹 보안모듈을 사용자 단말의 보안 클라이언트로 전송하여, 사용자 단말의 각종 응용 프로그램들에 대한 보안모듈이 수시로 변경되도록 함으로써, 상기 응용 프로그램들에 대한 해킹이 어려워지도록 하여 사용자 단말의 보안성(security)을 현저하게 향상시킬 수 있는 효과가 있다.

도면의 간단한 설명

[24] 도 1은 본 발명의 일실시예에 따른 다이나믹 보안모듈 서버장치의 개략적인 구성을 나타낸 모식도이다.

[25] 도 2은 본 발명의 일실시예에 따른 다이나믹 보안모듈 서버장치에서 다이나믹 보안모듈을 저장하는 모습을 나타낸 모식도이다.

[26] 도 3는 본 발명의 일실시예에 따른 다이나믹 보안모듈 서버장치에서 세션 아이디 및 다이나믹 보안모듈 파라미터 생성예를 나타낸 모식도이다.

[27] 도 4는 본 발명의 제1 실시예에 따른 다이나믹 보안모듈 서버장치의 구동방법을 나타낸 블록도이다.

[28] 도 5은 본 발명의 제2 실시예에 따른 다이나믹 보안모듈 서버장치의 구동방법을 나타낸 블록도이다.

[29] 도 6은 본 발명의 제3 실시예에 따른 다이나믹 보안모듈 서버장치의 구동방법을 나타낸 블록도이다.

발명의 실시를 위한 최선의 형태

[30] 이러한 목적을 달성하기 위하여 본 발명에 따른 다이나믹 보안모듈 서버장치는 사용자 단말에 다이나믹 보안모듈을 전송하며, 사용자 단말로부터 보안관리 이벤트를 수신하는 다이나믹 보안모듈 서버장치로서, 네트워크를 통해 상기 보안관리 이벤트를 송수신 하는 커뮤니케이션 유닛 및 상기 커뮤니케이션 유닛을 제어하는 프로세서를 포함하고, 상기 프로세서는 상기 사용자 단말의 보안 클라이언트와 보안 세션을 생성하고, 상기 다이나믹 보안모듈을 상기 사용자 단말의 보안 클라이언트로 전송하되, 상기 보안 세션이 생성된 상기 사용자 단말의 보안 클라이언트에서 상기 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 하는 것으로 구성된다.

[31] 상기 프로세서는 상기 보안 클라이언트로 전송된 다이나믹 보안모듈로부터 보안관리 결과를 수신하고, 상기 수신한 보안관리 결과를 확인하여, 보안관리 확인 결과값을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 것을 더 포함할 수 있다.

[32] 상기 프로세서는 상기 사용자 단말에 보안문제 발생 시, 상기 사용자 단말의 응용 프로그램을 정지시키도록 하는 정지명령을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 것을 더 포함할 수 있다.

[33] 상기 프로세서는 보안 세션 식별자로서 세션 아이디를 생성하여 저장하고, 상기 세션 아이디를 상기 보안 클라이언트에 전송하여 상기 보안 클라이언트가 상기 세션 아이디를 저장하도록 하여, 상기 보안 세션을 생성할 수 있다.

[34] 상기 보안 세션의 생성은 인증이 완료된 사용자 단말의 보안 클라이언트와 생성할 수 있다.

[35] 상기 유효시간은 상기 유효시간의 경과 시 상기 코드의 일부 또는 전부가 삭제되거나, 사용되지 않도록 하는 유효시간일 수 있다.

[36] 상기 프로세서는 상기 보안 세션이 유지되는 동안 상기 보안 클라이언트로 전송된 각각의 상기 다이나믹 보안모듈에 대한 파라미터를 저장되도록 하는 것을 더 포함할 수 있다.

[37] 상기 프로세서는 상기 보안 클라이언트로부터 전송된 내역이 상기 다이나믹 보안모듈의 파라미터의 구성과 동일한 지를 검증하는 것을 더 포함할 수 있다.

[38] 상기 다이나믹 보안모듈 서버장치는 상기 사용자 단말의 보안 클라이언트로 전송할 다이나믹 보안모듈, 보안 세션 식별자로서 세션 아이디, 및 다이나믹 보안모듈에 대한 파라미터를 저장하는 스토리지를 더 포함할 수 있다.

[39] 상기 프로세서는 상기 다이나믹 보안모듈이 정상 동작했음을 증명하는 검증토큰을 상기 사용자 단말의 응용 프로그램 운용서버로 전송하는 것을 더 포함할 수 있다.

[40] 본 발명은 또한, 상기 목적을 달성하기 위하여, 사용자 단말에 다이나믹 보안모듈을 전송하며, 사용자 단말로부터 보안관리 이벤트를 수신하는 다이나믹 보안모듈 서버장치의 구동방법으로서, 상기 사용자 단말의 보안 클라이언트와 보안 세션을 생성하는 단계 및 상기 다이나믹 보안모듈을 상기 보안 세션이 생성된 상기 사용자 단말의 보안 클라이언트에서 상기 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 상기 사용자 단말의 보안 클라이언트로 전송하는 단계를 포함하는 다이나믹 보안모듈 서버장치의 구동방법을 제공한다.

[41] 상기 구동방법은 상기 보안 클라이언트로 전송된 다이나믹 보안모듈로부터 보안관리 결과를 수신하고, 상기 수신한 보안관리 결과를 확인하여, 보안관리 확인 결과값을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계를 더 포함할 수 있다.

[42] 상기 구동방법은 상기 사용자 단말에 보안문제가 발생 시, 상기 사용자 단말의 응용 프로그램을 정지시키도록 하는 정지명령을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계를 더 포함할 수 있다.

[43] 상기 구동방법은 보안 세션 식별자로서 세션 아이디를 생성하여 저장하고, 상기 세션 아이디를 상기 보안 클라이언트에 전송하여 상기 보안 클라이언트가 상기 세션 아이디를 저장하도록 하여, 상기 보안 세션을 생성할 수 있다.

[44] 상기 구동방법은 상기 보안 세션이 유지되는 동안 상기 보안 클라이언트로 전송된 각각의 상기 다이나믹 보안모듈에 대한 파라미터를 저장하는 단계를 더 포함할 수 있다.

[45] 본 발명은 또한, 상기 다이나믹 보안모듈 서버장치의 구동방법을 실행하기 위한 프로그램이 기록되어 있는 컴퓨터에서 판독 가능한 기록 매체를 제공한다.

발명의 실시를 위한 형태

[46] 이하, 본 발명의 바람직한 실시예를 첨부된 도면들을 참조하여 상세히 설명한다. 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략하기로 한다. 또한 본 발명의 실시예들을 설명함에 있어 구체적인 수치는 실시예에 불과하다.

[47] 도 1에는 본 발명의 일실시예에 따른 다이나믹 보안모듈 서버장치의 개략적인 구성을 나타낸 모식도가 도시되어 있고, 도 2에는 본 발명의 일실시예에 따른

다이나믹 보안모듈 서버장치에서 다이나믹 보안모듈을 저장하는 모습을 나타낸 모식도가 도시되어 있으며, 도 3에는 본 발명의 일실시예에 따른 다이나믹 보안모듈 서버장치에서 세션 아이디 및 다이나믹 보안모듈 파라미터 생성예를 나타낸 모식도가 도시되어 있다.

[48] 이들 도면을 참조하면, 본 발명에 따른 다이나믹 보안모듈 서버장치(110)는 사용자 단말(150)에 다이나믹 보안모듈(118)을 전송하며, 사용자 단말(150)로부터 보안관리 이벤트를 수신하는 다이나믹 보안모듈 서버장치로서, 네트워크를 통해 상기 보안관리 이벤트를 송수신 하는 커뮤니케이션 유닛(112) 및 상기 커뮤니케이션 유닛(112)을 제어하는 프로세서(114)를 포함하고, 상기 프로세서(114)는 상기 사용자 단말(150)의 보안 클라이언트(152)와 보안 세션을 생성하고, 상기 다이나믹 보안모듈(118)을 상기 사용자 단말(150)의 보안 클라이언트(152)로 전송하되, 상기 보안 세션이 생성된 상기 사용자 단말(150)의 보안 클라이언트(152)에서 상기 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 하는 것으로 구성될 수 있다.

[49] 즉, 본 발명에 따른 다이나믹 보안모듈 서버장치(110)는 프로세서(114)가 사용자 단말(150)의 보안 클라이언트(152)에서 보안관리를 수행하는 코드의 일부 또는 전부가 일정한 유효시간을 가지는 다이나믹 보안모듈(118)들을 저장하거나, 전송 시마다 생성하여, 사용자 단말(150)의 구동 시, 또는 사용자 단말(150)에서 상기 보안 클라이언트(152)를 포함하는 응용 프로그램의 구동 시, 또는 사용자 단말(150)의 사용자 요청 시, 또는 상기 다이나믹 보안모듈 서버장치(110)에서 설정한 일정 주기마다, 또는 사용자 단말(150)에서 설정한 일정 주기마다 등의 다양한 경우에 사용자 단말(150)의 보안 클라이언트(152)와 보안 세션을 생성하여, 상기 다이나믹 보안모듈(118)을 상기 사용자 단말(150)의 보안 클라이언트(152)로 전송함으로써, 상기 다이나믹 보안모듈(118)이 자주 갱신되도록 하여, 보안모듈의 해킹이나 컴퓨터 바이러스 감염 등으로 인한 사용자 단말에 탑재된 응용 프로그램들에 대한 보안문제 발생을 효과적으로 방지할 수 있는 특징이 있다.

[50] 또한, 상기 다이나믹 보안모듈(118)은 같은 종류의 다이나믹 보안모듈을 반복해서 상기 보안 클라이언트(152)로 전송하지 않고, 예를 들어, 보안관리를 수행하기 위한 코드의 함수명, 실행될 알고리즘을 지정하는 변수, 프로토콜 필드, 프로토콜 시퀀스를 지정하는 변수, 컴파일 레벨을 지정하는 변수 및 실행 코드 난독화 방법을 지정하는 변수로 이루어진 군에서 선택된 1종 이상의 변경 가능한 부분을 다르게 구성하여 서로 다른 코드 구조 또는 알고리즘을 갖는 적어도 2가지 이상의 다이나믹 보안모듈을 상기 프로세서(114)저장하여 두고, 상기 보안 클라이언트(152)로의 전송 시 마다 각각 다른 다이나믹 보안모듈(118)을 선택하여 전송할 수 있다.

[51] 또한, 상기 다이나믹 보안모듈(118)의 보안관리를 수행하는 코드의 일부 또는 전부의 유효시간은 예를 들어, 1시간, 3시간, 6시간, 9시간, 12시간, 24시간,

48시간 및 72 시간으로 이루어진 군에서 선택된 시간 간격으로 설정하여 이러한 설정시간이 종료되었을 경우, 다이나믹 보안모듈(118)의 코드의 일부 또는 전부의 기능이 정지하도록 구성할 수도 있다. 따라서, 이와 같은 다이나믹 보안모듈(118)의 유효시간 만료 시, 상기 보안 클라이언트(152)는 다이나믹 보안모듈(118)에 대한 사용을 중지하고, 상기 다이나믹 보안모듈 서버장치(110)로부터 새로운 다이나믹 보안모듈(118)을 전송 받아 갱신함으로써, 다이나믹 보안모듈(118)의 해킹이나 바이러스 감염으로 인한 상기 사용자 단말(150)의 보안문제 발생을 효과적으로 방지할 수 있다.

[52] 여기서, 보안관리는 상기 다아나믹 보안모듈(118)이 상기 보안 클라이언트(152)를 포함하는 응용 프로그램에 대한 해킹 위협이 될 수 있는 요소의 존재 여부를 감지하는 것, 상기 응용 프로그램이 설치된 단말기의 O/S 위변조, 앱(App)의 위변조, 루팅(Rooting), 디버거(debugger), 루트 프로세스 실행이력, 유해 어플리케이션 설치, 유해 어플리케이션 실행이력, 유해 포트, 세션 위변조, 입력값 위변조 및 컴퓨터 바이러스로 이루어진 해킹 위협이 될 수 있는 요소를 검출하는 것, 상기 해킹 위협이 될 수 있는 요소에 대한 정보를 상기 다이나믹 보안모듈 서버장치(110)로 전송하는 것, 상기 응용 프로그램에 대한 바이러스를 치료하는 것, 상기 용응 프로그램에 대한 해킹 위협과 바이러스 감염문제를 방지하기 위해 상기 응용 프로그램에 대한 정지명령을 전송하는 것, 상기 다아나믹 보안모듈(118)의 유효시간 만료 또는 해커에 의한 해킹, 바이러스 감염 등의 문제로 인해 다이나믹 보안모듈(118) 자체의 기능을 정지하는 것 등과 같은 상기 다이나믹 보안모듈(118)이 상기 사용자 단말(150)의 보안을 위해 수행하는 전반적인 관리를 포함하는 개념이다.

[53] 또한, 상기 사용자 단말(150)로부터 수신된 보안관리 이벤트는 예를 들어, 상기 보안 클라이언트(152)로부터 전송된 다이나믹 보안모듈(118)에 대한 파라미터를 판단하기 위한 내역, 다이나믹 보안모듈(118)이 구동되고 있는 상태에 대한 스테이트(state) 내역, 해킹 위협이 있었음을 알리는 보안관리 결과 정보, 및 상기 사용자 단말(150)에 탑재된 응용 프로그램에 대한 바이러스 치료 내역 등의 다양한 이벤트일 수 있다.

[54] 또한, 상기 사용자 단말(150)은 예를 들어, 스마트폰, 테블릿 PC, 데스크 톱 컴퓨터, 노트북 컴퓨터 등의 보안이 필요한 다양한 단말기기 일 수 있다.

[55] 상기 프로세서(114)는 제어 신호를 생성하여 커뮤니케이션 유닛(112)과 스토리지(113)를 포함하는 상기 서버장치(110)를 제어할 수 있다. 여기서, 커뮤니케이션 유닛(112)은 외부 디바이스와 다양한 프로토콜을 이용하여 통신을 수행하여 데이터를 송수신할 수 있으며, 유선 또는 무선으로 외부 네트워크에 접속하여, 컨텐츠, 애플리케이션 등의 디지털 데이터를 송수신할 수 있다.

[56] 또한, 상기 스토리지(113)는 오디오, 사진, 동영상, 애플리케이션 등을 포함하는 다양한 디지털 데이터를 저장할 수 있는 장치로서, 플래시 메모리, RAM(Random Access Memory), SSD(Solid State Drive) 등의 다양한 디지털 데이터 저장 공간을

나타낸다. 이러한 스토리지(113)는 커뮤니케이션 유닛(112)을 통해 외부 디바이스로부터 수신된 데이터를 임시적으로 저장할 수 있다.

[57] 상기 프로세서(114)는 상기 보안 클라이언트(152)로 전송된 다이나믹 보안모듈(118)로부터 보안관리 결과를 수신하고, 상기 수신한 보안관리 결과를 확인하여, 보안관리 확인 결과값을 상기 보안 클라이언트(152)의 다이나믹 보안모듈(118)로 전송하는 것을 더 포함할 수 있다.

[58] 여기서, 상기 보안관리 결과는 상기 다이나믹 보안모듈(118)이 상기 보안 클라이언트(152)에서 실제 수행한 보안관리의 내역으로서, 상기 다이나믹 보안모듈(118)에 포함되어 있는 세부적인 보안관리 기능들을 수행한 결과값이며, 보안관리 이벤트의 일부분이다. 예를 들어, 상기 해킹 위협이 될 수 있는 요소의 존재 여부에 대한 감지 결과, 상기 해킹 위협이 될 수 있는 요소를 검출 결과, 상기 응용 프로그램에 대한 바이러스 치료 및 해킹 위협이 될 수 있는 요소의 제거 결과 등의 내역일 수 있다.

[59] 또한, 상기 보안관리 확인 결과값은 상기 다이나믹 보안모듈 서버장치(110)가 상기 보안관리 결과를 수신하여, 상기 보안관리 결과를 기초로 분석한 상기 사용자 단말(150)의 보안문제 발생여부에 대한 판단결과이다. 즉, 상기 사용자 단말(150)에 현재 해킹 위협이 될 수 있는 요소가 존재 하는지에 대한 판단결과, 사용자 단말(150)에 탑재된 응용 프로그램이 해킹되었는지에 대한 판단결과, 및 상기 응용 프로그램이 바이러스나, 악성코드에 감염되었는지에 대한 판단결과일 수 있다.

[60] 구체적으로, 상기 보안 클라이언트(152)로 전송된 다이나믹 보안모듈(118)로부터 상기 보안관리로서 보안관리 결과를 수신하고, 상기 수신한 보안관리 결과를 확인하여, 상기 사용자 단말(150)에 보안문제가 발생하지 않은 경우, 보안문제가 발생하지 않았음을 알리는 보안진단 확인 결과값을 상기 보안 클라이언트(152)의 다이나믹 보안모듈(118)로 전송하는 것을 더 포함할 수 있다.

[61] 또한, 상기 보안 클라이언트(152)로 전송된 다이나믹 보안모듈(118)로부터 상기 보안관리로서 보안관리 결과를 수신하고, 상기 수신한 보안관리 결과를 확인하여, 상기 사용자 단말(150)에 보안문제가 발생한 경우, 보안문제가 발생하였음을 알리는 보안관리 확인 결과값을 상기 보안 클라이언트(152)의 다이나믹 보안모듈(118)로 전송하는 것을 더 포함할 수 있다.

[62] 즉, 본 발명에 따른 다이나믹 보안모듈 서버장치(110)는 사용자 단말(150)의 보안 클라이언트(152)로 전송한 다이나믹 보안모듈(118)로부터 보안관리 결과를 수신하여 이를 확인하고, 보안관리 확인 결과값을 다시 다이나믹 보안모듈(118)로 전송함으로써, 다이나믹 보안모듈(118)이 상기 사용자 단말(150)의 보안문제 발생시 신속하고 효과적으로 대처하도록 할 수 있다.

[63] 이와 관련하여, 상기 프로세서(114)는 상기 보안 클라이언트(152)로 전송된 다이나믹 보안모듈(118)로부터 상기 보안관리로서 보안관리 결과를 수신하고,

상기 수신한 보안관리 결과를 확인하여, 상기 사용자 단말에 보안문제가 발생한 경우, 상기 사용자 단말(150)의 응용 프로그램을 정지시키도록 하는 정지명령을 상기 보안 클라이언트(152)의 다이나믹 보안모듈(118)로 전송하고, 상기 보안 클라이언트(152)와의 보안 세션을 파기하는 것을 더 포함함으로써, 해커가 다이나믹 보안모듈(118)을 해킹하여 사용자 단말(150)의 각종 응용 프로그램들에 대한 보안문제를 발생시키는 문제를 근본적으로 방지할 수 있다.

[64] 즉, 상기 사용자 단말(150)의 보안문제 발생시, 상기 사용자 단말(150)에 탑재된 응용 프로그램의 구동을 신속하게 정지하도록 함으로써, 상기 응용 프로그램의 구동에 의한 상기 사용자 단말(150)에 탑재된 다른 응용 프로그램들에 대한 추가적인 보안문제의 확산을 방지하고, 상기 보안 세션을 파기하여 해커에 의한 다이나믹 보안모듈(118) 또는 다이나믹 보안모듈 서버장치(110)에 대한 추적 및 분석을 신속하게 차단할 수 있다.

[65] 한편, 상기 프로세서(114)는 보안 세션 식별자로서 세션 아이디(116)를 생성하여 저장하고, 상기 세션 아이디(116)를 상기 보안 클라이언트(152)에 전송하여 상기 보안 클라이언트(152)가 상기 세션 아이디(116)를 저장하도록 함으로써, 보안 세션을 생성할 수 있다. 이러한 세션 아이디를 이용하여 보안 세션을 생성하는 방법은 여러 개의 보안 세션을 생성하여 보안 세션을 자주 갱신함으로써, 상기 다이나믹 보안모듈(118)에 의한 상기 사용자 단말(150)에 대한 보안관리의 신뢰성과 편의성을 향상시킬 수 있는 장점이 있다.

[66] 여기서, 상기 보안 세션의 생성은 인증이 완료된 사용자 단말의 보안 클라이언트(152)와 생성하는 것으로 이루어질 수 있다. 즉, 상기 보안 세션의 생성은 사용자 단말에 대한 보안성을 한 단계 더 향상시킬 수 있도록, 다이나믹 보안모듈(118)을 전송하기 위한 사용자 단말(150)의 보안 클라이언트(152)에 대한 인증 과정을 더 수행할 수 있다.

[67] 또한, 상기 사용자 단말(150)의 보안 클라이언트(152)의 인증은 예를 들어, 상기 보안 클라이언트(152)가 포함된 응용 프로그램인 어플리케이션이 상기 사용자 단말(150)에 설치됨과 동시에 인증이 완료되거나, 또는 상기 어플리케이션이 상기 사용자 단말(150)에 설치된 후, 최초 구동 시 인증이 완료되거나, 또는 상기 어플리케이션에 대한 로그인(log in) 및 로그아웃(log out) 시 인증이 완료되거나, 또는 상기 어플리케이션이 상기 사용자 단말(150)에 설치된 후, 상기 어플리케이션을 통한 사용자의 요청에 의해 인증이 완료될 수 있다.

[68] 상기 유효시간은 상기 유효시간의 경과 시 상기 코드의 일부 또는 전부가 삭제되거나, 사용되지 않도록 하는 유효시간일 수 있다. 즉, 상기 사용자 단말(150)의 보안 클라이언트(152)에서 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 갖는 상기 다이나믹 보안모듈(118)은 유효시간의 경과 시 코드의 일부 또는 전부가 삭제되거나, 보안관리를 수행하지 않도록 다이나믹 보안모듈 자체의 사용이 중지될 수 있다.

[69] 따라서, 이러한 다이나믹 보안모듈(118)의 유효시간 만료시, 상기 보안

클라이언트(152)는, 다이나믹 보안모듈(118)을 구성하는 코드의 일부 또는 전부를 갱신함으로써, 다이나믹 보안모듈(118)의 해킹이나 바이러스의 감염 등의 원인에 의한 보안문제 발생을 원천적으로 차단할 수 있다.

[70] 또한, 상기 프로세서(114)는 상기 보안 세션이 유지되는 동안 상기 보안 클라이언트(152)로 전송된 각각의 상기 다이나믹 보안모듈(118)에 대한 파라미터를 저장하는 것을 더 포함할 수 있다.

[71] 여기서, 다이나믹 보안모듈(118)에 대한 파라미터는 상기 보안 클라이언트(152)로 전송되 보안관리를 수행하고 있는 다이나믹 보안모듈의 보안관리를 수행하기 위한 코드의 함수명, 실행될 알고리즘을 지정하는 변수, 프로토콜 필드, 프로토콜 시퀀스를 지정하는 변수, 컴파일 레벨을 지정하는 변수 및 실행 코드 난독화 방법을 지정하는 변수 등에 대한 구체적인 정보에 관한 것으로, 자주 갱신되어 서로 다른 구성을 갖는 각각의 다이나믹 보안모듈들을 서로 구분하기 위한 것이며, 상기 다이나믹 보안모듈 서버장치(110)에서 결정되는 정보로서, 상기 다이나믹 보안모듈(118)의 보안관리를 수행하는 코드의 실행 시의 정보이다.

[72] 또한, 상기 프로세서(114)는 상기 보안 클라이언트(152)로 전송된 다이나믹 보안모듈(118)들에 대한 내역을 수신하여, 상기 저장한 다이나믹 보안모듈(118)의 파라미터의 구성과 동일한 지를 검증하는 것을 더 포함할 수 있다. 이러한 다이나믹 보안모듈의 파라미터의 변경 내용 검증은 예를 들어, 각각의 파라미터가 A-B-C-D와 같이 순차적으로 전송된 다이나믹 보안모듈들의 파라미터가 상기 보안 클라이언트(152)로부터 전송된 내역과 비교했을 때, 동일하지 않고 다르게 변경된 것으로 확인된 경우, 해커에 의한 해킹 시도 등이 있었음을 유추할 수 있으며, 이에 대한 조치를 수행할 수 있다.

[73] 구체적으로, 도 4에서와 같이 상기 다이나믹 보안모듈 서버장치(110)와 사용자 단말(150)의 보안 클라이언트(152)가 세션 아이디로서 11836381를 생성하여 보안 세션을 생성한 경우, 상기 보안 클라이언트(152)로부터 전송된 다이나믹 보안모듈(118)에 대한 내역이 파라미터(param)는 A, B, C 이고, 이때의 스테이트(state)가 1, 2 임을 검증하고, 세션 아이디로서 72365784를 생성하여 보안 세션을 생성한 경우, 보안 클라이언트(152)로부터 전송된 다이나믹 보안모듈(118)에 대한 내역이 파라미터(param)는 C, B, A 이고, 이때의 스테이트(state)가 0, 3 임을 검증하며, 세션 아이디로서 87656501를 생성하여 보안 세션을 생성한 경우, 보안 클라이언트(152)로부터 전송된 다이나믹 보안모듈(118)에 대한 내역이 파라미터(param)는 B, A, C 이고, 이때의 스테이트(state)가 3, 2 임을 검증할 수 있다. 여기서, 이러한 파라미터와 스테이트 내역은 상기 사용자 단말(150)로부터 수신된 보안관리 이벤트일 수 있다.

[74] 상기 보안관리는 상기 보안 클라이언트(152)로 전송된 각각의 다이나믹 보안모듈(118)의 프로토콜 필드 및 프로토콜 시퀀스를 저장하고, 상기 보안 클라이언트(152)에서의 상기 다이나믹 보안모듈(118)의 프로토콜 필드 및

프로토콜 시퀀스를 수신하여 상기 저장된 프로토콜 필드 및 프로토콜 시퀀스와 상기 수신한 프로토콜 필드 및 프로토콜 시퀀스를 서로 비교하여 검증하는 것일 수 있다.

[75] 즉, 상기 보안관리는 상기 보안 클라이언트(152)로 전송된 다이나믹 보안모듈(118)들의 프로토콜 필드 및 프로토콜 시퀀스를 수신하여 분석함으로써, 프로토콜 진행에 예를 들어, 적어도 1번 이상의 오류가 발생할 경우, 해커에 의한 해킹 시도 등이 있었음을 유추할 수 있다. 따라서, 이러한 다이나믹 보안모듈(118)의 프로토콜 필드 및 프로토콜 시퀀스의 분석 내용을 기초로 해킹 위험이나 보안문제 발생 가능성을 예측하고, 보안문제가 발생하지 않도록 조치할 수 있다.

[76] 여기서, 상기 프로토콜 필드는 상기 다이나믹 보안모듈(118)이 상기 보안 클라이언트(152)에서 수행하는 보안관리의 다양한 항목들에 대한 수행방법 등의 규약으로서 예를 들어, 상기 보안 클라이언트(152)를 포함하는 응용 프로그램에 대한 해킹 위협이 될 수 있는 요소의 존재 여부를 판별한 결과를 전송하는 통신 규약, 상기 응용 프로그램에 대한 파일 바이러스, 부트 앤 파일(Boot & file) 바이러스 등에 대한 자체 치료 내역을 전송하는 통신 규약일 수 있다.

[77] 또한, 상기 프로토콜 시퀀스는 상기 다이나믹 보안모듈(118)이 상기 보안 클라이언트(152)에서 수행하는 보안관리를 포함하는 다양한 항목들에 대한 수행순서를 의미하는 것으로서, 예를 들어, 상기 응용프로그램이 설치된 단말기의 O/S 위변조, 앱(App)의 위변조, 루팅(Rooting), 디버거(debugger), 루트 프로세스 실행이력, 유해 어플리케이션 설치, 유해 어플리케이션 실행이력, 유해 포트, 세션 위변조, 입력값 위변조 및 컴퓨터 바이러스로 이루어진 해킹 위협이 될 수 있는 요소의 검출에 있어서, 상기 각각의 요소들을 검출하는 순서일 수 있다.

[78] 상기 다이나믹 보안모듈 서버장치(110)는 상기 사용자 단말(150)의 보안 클라이언트(152)로 전송할 다이나믹 보안모듈(118), 보안 세션 식별자로서 세션 아이디(116), 및 다이나믹 보안모듈에 대한 파라미터를 저장하는 스토리지(113)를 더 포함할 수 있다.

[79] 즉, 상기 다이나믹 보안모듈 서버장치(110)는 상기 스토리지(113)에 다이나믹 보안모듈(118), 세션 아이디(116)를 저장함으로써, 상기 다이나믹 보안모듈(118)과 세션 아이디(116)를 원활하고 안정적으로 상기 보안 클라이언트(152)로 전송할 수 있다. 또한, 상기 스토리지(113)에 상기 보안 클라이언트(152)로 전송한 다이나믹 보안모듈에 대한 파라미터를 저장함으로써, 상기 보안 클라이언트(152)로 전송된 다이나믹 보안모듈(118)에 대한 수신 내역과의 동일성 검증을 더욱 안정적으로 수행할 수 있다.

[80] 상기 프로세서(114)는 상기 다이나믹 보안모듈(118)이 정상 동작했음을 증명하는 검증토큰을 상기 사용자 단말(150)의 응용 프로그램 운용서버로 전송하는 것을 더 포함할 수 있다.

[81] 구체적으로, 상기 프로세서(114)는 상기 다이나믹 보안모듈(118)로부터 수신한 보안관리 결과를 확인하여, 상기 사용자 단말(150)에 보안문제가 발생하지 않은 경우, 상기 보안관리 확인 결과값이 상기 보안 클라이언트(152)를 우회하지 않았음을 증명하는 검증토큰을 포함시켜 상기 보안관리 확인 결과값을 상기 다이나믹 보안모듈(118)로 전송하고, 상기 다이나믹 보안모듈(118)은 상기 보안 클라이언트(152)를 포함하는 응용 프로그램의 운용서버(도시하지 않음)로 상기 검증토큰을 전송하며, 상기 운용서버는 상기 검증토큰을 상기 다이나믹 보안모듈 서버장치(110) 프로세서(114)에 다시 전송하여 상기 검증토큰이 유효한지를 검증하도록 하는 과정을 더 수행할 수 있다.

[82] 즉, 상기 다이나믹 보안모듈 서버장치(110)는 상기 보안관리 확인 결과값과 함께 상기 보안관리 확인 결과값에 대한 검증 토큰을 추가하여 상기 다이나믹 보안모듈(118)로 전송하고, 상기 다이나믹 보안모듈(118)은 상기 보안 클라이언트(152)를 포함하는 응용 프로그램의 운용서버(도시하지 않음)로 상기 검증토큰을 전송함으로써, 상기 응용 프로그램의 운용서버로 하여금 상기 검증토큰을 통해 상기 보안관리 확인 결과값이 위, 변조 되지 않고 유효 한지의 여부를 검증하도록 하여 상기 보안관리 확인 결과값에 대한 신뢰도를 더욱 향상시킬 수 있다.

[83] 이때, 상기 다이나믹 보안모듈 서버장치(110)와 상기 응용 프로그램의 운용서버는 다이나믹 보안모듈 서버장치의 시스템 설계에 따라 하나의 서버로 병합하여 구성할 수도 있으며, 서로 분리되어 이격된 장소에 각각 따로 배치된 서버들로 구성하여 운영할 수도 있다.

[84]

[85] 도 4에는 본 발명의 제1 실시예에 따른 다이나믹 보안모듈 서버장치의 구동방법을 나타낸 블록도가 도시되어 있고, 도 5에는 본 발명의 제2 실시예에 따른 다이나믹 보안모듈 서버장치의 구동방법을 나타낸 블록도가 도시되어 있으며, 도 6에는 본 발명의 제3 실시예에 따른 다이나믹 보안모듈 서버장치의 구동방법을 나타낸 블록도가 도시되어 있다.

[86] 이들 도면을 참조하면, 우선 제1 실시예에 따른 다이나믹 보안모듈 서버장치의 구동방법은 사용자 단말에 상기 다이나믹 보안모듈을 전송하며, 사용자 단말로부터 보안관리 이벤트를 수신하는 다이나믹 보안모듈 서버장치의 구동방법으로서, 상기 사용자 단말의 보안 클라이언트와 보안 세션을 생성하는 단계(S210), 및 상기 다이나믹 보안모듈을 상기 보안 세션이 생성된 상기 사용자 단말의 보안 클라이언트에서 상기 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 상기 사용자 단말의 보안 클라이언트로 전송하는 단계(S220)로 수행된다.

[87] 이후, 상기 보안 클라이언트로 전송된 다이나믹 보안모듈로부터 상기 보안관리로서 보안관리 결과를 수신하는 단계(S230), 상기 수신한 보안관리 결과를 확인하여 보안문제 발생여부를 확인하는 단계(S240), 및 상기 사용자

단말에 보안문제가 발생하지 않은 경우, 보안문제가 발생하지 않았음을 알리는 보안관리 확인 결과값을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계(S250)로 수행된다.

[88] 여기서, 상기 사용자 단말에 보안문제가 발생한 경우에는, 보안문제가 발생하였음을 알리는 보안관리 확인 결과값을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계(S251)가 수행된다.

[89] 또한, 상기 사용자 단말에 보안문제가 발생한 경우, 상기 사용자 단말의 응용 프로그램을 정지시키도록 하는 정지명령을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계(S252)가 더 수행될 수 있다.

[90] 제2 실시예에 따른 본원발명의 다이나믹 보안모듈 서버장치의 구동방법은 사용자 단말에 상기 다이나믹 보안모듈을 전송하며, 사용자 단말로부터 보안관리 이벤트를 수신하는 다이나믹 보안모듈 서버장치의 구동방법으로서, 상기 사용자 단말의 보안 클라이언트와 보안 세션을 생성하는 단계(S310), 상기 다이나믹 보안모듈을 상기 보안 세션이 생성된 상기 사용자 단말의 보안 클라이언트에서 상기 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 상기 사용자 단말의 보안 클라이언트로 전송하는 단계(S320), 상기 보안 세션에 대한 유효시간을 설정하여, 상기 유효시간 정보를 상기 보안 세션이 생성된 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계(S330) 및 상기 보안 세션의 유효시간 종료에 의한 보안 세션 종료 시, 상기 다이나믹 보안모듈에 대한 폐기명령을 상기 다이나믹 보안모듈 또는 상기 보안 클라이언트로 전송하는 단계(S340)로 수행될 수 있다.

[91] 이때, 상기 보안 세션에 대한 유효시간은 예를 들어, 1시간, 3시간, 6시간, 9시간, 12시간, 24시간, 48시간 및 72 시간으로 이루어진 군에서 선택된 시간 간격으로 설정하여 상기 다이나믹 보안모듈로 전송할 수 있다.

[92] 제3 실시예에 따른 본원발명의 다이나믹 보안모듈 서버장치의 구동방법은 사용자 단말에 상기 다이나믹 보안모듈을 전송하며, 사용자 단말로부터 보안관리 이벤트를 수신하는 다이나믹 보안모듈 서버장치의 구동방법으로서, 사용자 단말의 보안 클라이언트와 보안 세션을 생성하는 단계(S410), 상기 다이나믹 보안모듈을 상기 보안 세션이 생성된 상기 사용자 단말의 보안 클라이언트에서 상기 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 상기 사용자 단말의 보안 클라이언트로 전송하는 단계(S420)로 수행된다.

[93] 이후, 상기 보안 세션이 유지되는 동안 상기 보안 클라이언트로 전송된 각각의 상기 다이나믹 보안모듈에 대한 파라미터를 저장하고, 상기 다이나믹 보안모듈의 상기 보안 클라이언트에서의 파라미터 변경내역을 수신하여 저장하는 단계(S430), 상기 다이나믹 보안모듈의 파라미터 변경내역으로부터 보안문제의 발생여부를 판단하는 단계(S440) 및 상기 사용자 단말에 보안문제가 발생하지 않은 경우, 보안문제가 발생하지 않았음을 알리는 보안관리 확인

결과값을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계(S450)로 수행된다.

[94] 여기서, 상기 사용자 단말에 보안문제가 발생한 경우에는, 보안문제가 발생하였음을 알리는 보안관리 확인 결과값을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계(S451)가 수행된다.

[95] 또한, 상기 사용자 단말에 보안문제가 발생한 경우, 상기 사용자 단말의 응용 프로그램을 정지시키도록 하는 정지명령을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계(S452)가 더 수행될 수 있다.

[96]

[97] 본 발명에 따른 다이나믹 보안모듈 서버장치의 구동방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[98]

[99] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[100] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

산업상 이용가능성

[101] 본 발명은 사용자 단말에 다이나믹 보안모듈을 전송하며, 사용자 단말로부터 보안관리 이벤트를 수신하는 다이나믹 보안모듈 서버장치로서, 네트워크를 통해 상기 보안관리 이벤트를 송수신 하는 커뮤니케이션 유닛 및 상기 커뮤니케이션 유닛을 제어하는 프로세서를 포함하고, 상기 프로세서는, 상기 사용자 단말의 보안 클라이언트와 보안 세션을 생성하고, 상기 다이나믹 보안모듈을 상기 사용자 단말의 보안 클라이언트로 전송하되, 상기 보안 세션이 생성된 상기 사용자 단말의 보안 클라이언트에서 상기 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 하는 다이나믹 보안모듈 서버장치에 관한 것이다.

[102] 본 발명에 따르면, 보안관리를 수행하는 코드의 일부 또는 전부가 일정한 유효시간을 가지는 다이나믹 보안모듈을 사용자 단말의 보안 클라이언트로

전송하여, 사용자 단말의 각종 응용 프로그램들에 대한 보안모듈이 수시로 변경되도록 함으로써, 상기 응용 프로그램들에 대한 해킹이 어려워지도록 하여 사용자 단말의 보안성(security)을 현저하게 향상시킬 수 있는 효과가 있다.

청구범위

[청구항 1] 사용자 단말에 다이나믹 보안모듈을 전송하며, 사용자 단말로부터 보안관리 이벤트를 수신하는 다이나믹 보안모듈 서버장치로서,
네트워크를 통해 상기 보안관리 이벤트를 송수신 하는 커뮤니케이션 유닛; 및
상기 커뮤니케이션 유닛을 제어하는 프로세서; 를 포함하고,
상기 프로세서는,
상기 사용자 단말의 보안 클라이언트와 보안 세션을 생성하고,
상기 다이나믹 보안모듈을 상기 사용자 단말의 보안 클라이언트로 전송하되,
상기 보안 세션이 생성된 상기 사용자 단말의 보안 클라이언트에서 상기 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 하는 다이나믹 보안모듈 서버장치.

[청구항 2] 제 1항에 있어서,
상기 프로세서는
상기 보안 클라이언트로 전송된 다이나믹 보안모듈로부터 보안관리 결과를 수신하고, 상기 수신한 보안관리 결과를 확인하여, 보안관리 확인 결과값을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 것을 더 포함하는 다이나믹 보안모듈 서버장치.

[청구항 3] 제 1항에 있어서,
상기 프로세서는
상기 사용자 단말에 보안문제 발생 시, 상기 사용자 단말의 응용 프로그램을 정지시키도록 하는 정지명령을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 것을 더 포함하는 다이나믹 보안모듈 서버장치.

[청구항 4] 제 1항에 있어서,
상기 프로세서는
보안 세션 식별자로서 세션 아이디를 생성하여 저장하고, 상기 세션 아이디를 상기 보안 클라이언트에 전송하여 상기 보안 클라이언트가 상기 세션 아이디를 저장하도록 하여, 상기 보안 세션을 생성하는 다이나믹 보안모듈 서버장치.

[청구항 5] 제 1항에 있어서,
상기 보안 세션의 생성은 인증이 완료된 사용자 단말의 보안 클라이언트와 생성하는 다이나믹 보안모듈 서버장치.

[청구항 6] 제 1항에 있어서,
상기 유효시간은 상기 유효시간의 경과 시 상기 코드의 일부 또는

전부가 삭제되거나, 사용되지 않도록 하는 유효시간인 다이나믹 보안모듈 서버장치.

[청구항 7] 제 1항에 있어서,
상기 프로세서는
상기 보안 세션이 유지되는 동안 상기 보안 클라이언트로 전송된 각각의 상기 다이나믹 보안모듈에 대한 파라미터를 저장되도록 하는 것을 더 포함하는 다이나믹 보안모듈 서버장치.

[청구항 8] 제 7항에 있어서,
상기 프로세서는
상기 보안 클라이언트로부터 전송된 내역이 상기 다이나믹 보안모듈의 파라미터의 구성과 동일한 지를 검증하는 것을 더 포함하는 다이나믹 보안모듈 서버장치.

[청구항 9] 제 1항에 있어서,
상기 다이나믹 보안모듈 서버장치는 상기 사용자 단말의 보안 클라이언트로 전송할 다이나믹 보안모듈, 보안 세션 식별자로서 세션 아이디, 및 다이나믹 보안모듈에 대한 파라미터를 저장하는 스토리지를 더 포함하는 다이나믹 보안모듈 서버장치.

[청구항 10] 제 1항에 있어서,
상기 프로세서는
상기 다이나믹 보안모듈이 정상 동작했음을 증명하는 검증토큰을 상기 사용자 단말의 응용 프로그램 운용서버로 전송하는 것을 더 포함하는 다이나믹 보안모듈 서버장치.

[청구항 11] 사용자 단말에 다이나믹 보안모듈을 전송하며, 사용자 단말로부터 보안관리 이벤트를 수신하는 다이나믹 보안모듈 서버장치의 구동방법으로서,
상기 사용자 단말의 보안 클라이언트와 보안 세션을 생성하는 단계; 및
상기 다이나믹 보안모듈을 상기 보안 세션이 생성된 상기 사용자 단말의 보안 클라이언트에서 상기 보안관리를 수행하는 코드의 일부 또는 전부가 유효시간을 가지도록 상기 사용자 단말의 보안 클라이언트로 전송하는 단계;
를 포함하는 다이나믹 보안모듈 서버장치의 구동방법.

[청구항 12] 제 11항에 있어서,
상기 구동방법은
상기 보안 클라이언트로 전송된 다이나믹 보안모듈로부터 보안관리 결과를 수신하고, 상기 수신한 보안관리 결과를 확인하여, 보안관리 확인 결과값을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계를 더 포함하는 다이나믹

보안모듈 서버장치의 구동방법.

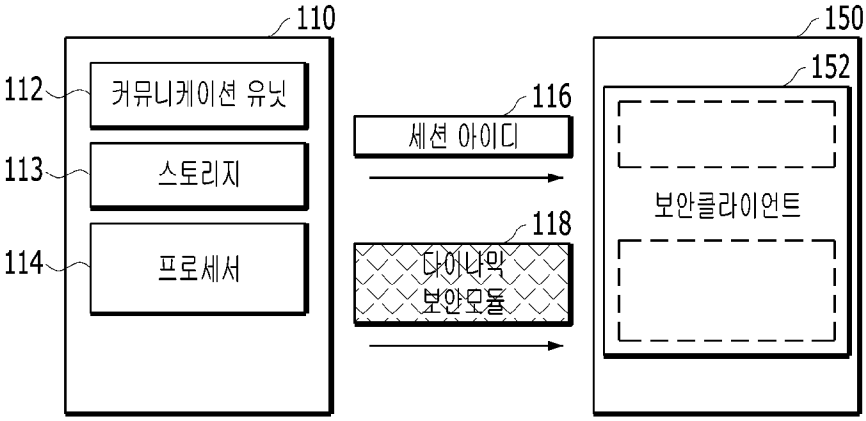
[청구항 13] 제 11항에 있어서,
상기 구동방법은
상기 사용자 단말에 보안문제가 발생 시, 상기 사용자 단말의 응용 프로그램을 정지시키도록 하는 정지명령을 상기 보안 클라이언트의 다이나믹 보안모듈로 전송하는 단계를 더 포함하는 다이나믹 보안모듈 서버장치의 구동방법.

[청구항 14] 제 11항에 있어서,
상기 구동방법은
보안 세션 식별자로서 세션 아이디를 생성하여 저장하고, 상기 세션 아이디를 상기 보안 클라이언트에 전송하여 상기 보안 클라이언트가 상기 세션 아이디를 저장하도록 하여, 상기 보안 세션을 생성하는 다이나믹 보안모듈 서버장치의 구동방법.

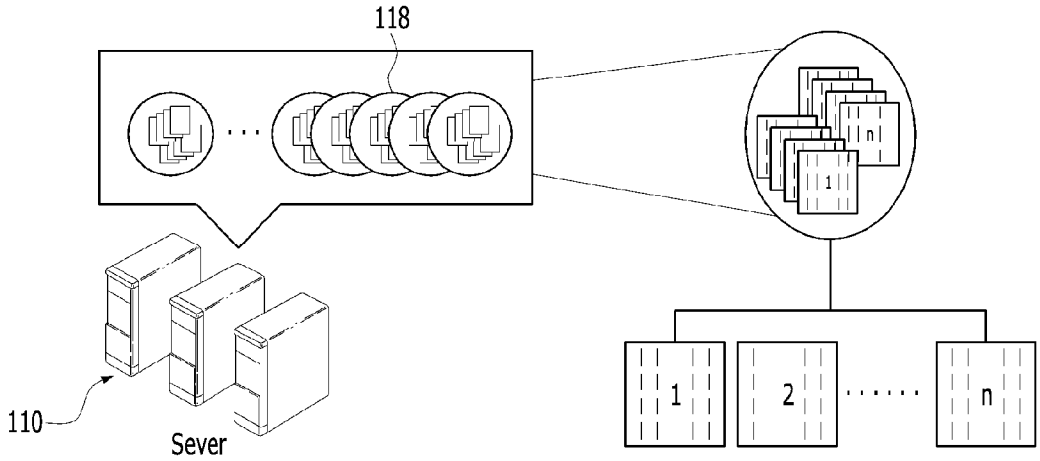
[청구항 15] 제 11항에 있어서,
상기 구동방법은
상기 보안 세션이 유지되는 동안 상기 보안 클라이언트로 전송된 각각의 상기 다이나믹 보안모듈에 대한 파라미터를 저장하는 단계를 더 포함하는 다이나믹 보안모듈 서버장치의 구동방법.

[청구항 16] 제11항 내지 제15항 중 어느 한 항의 방법을 실행하기 위한 프로그램이 기록되어 있는 컴퓨터에서 판독 가능한 기록 매체.

[Fig. 1]



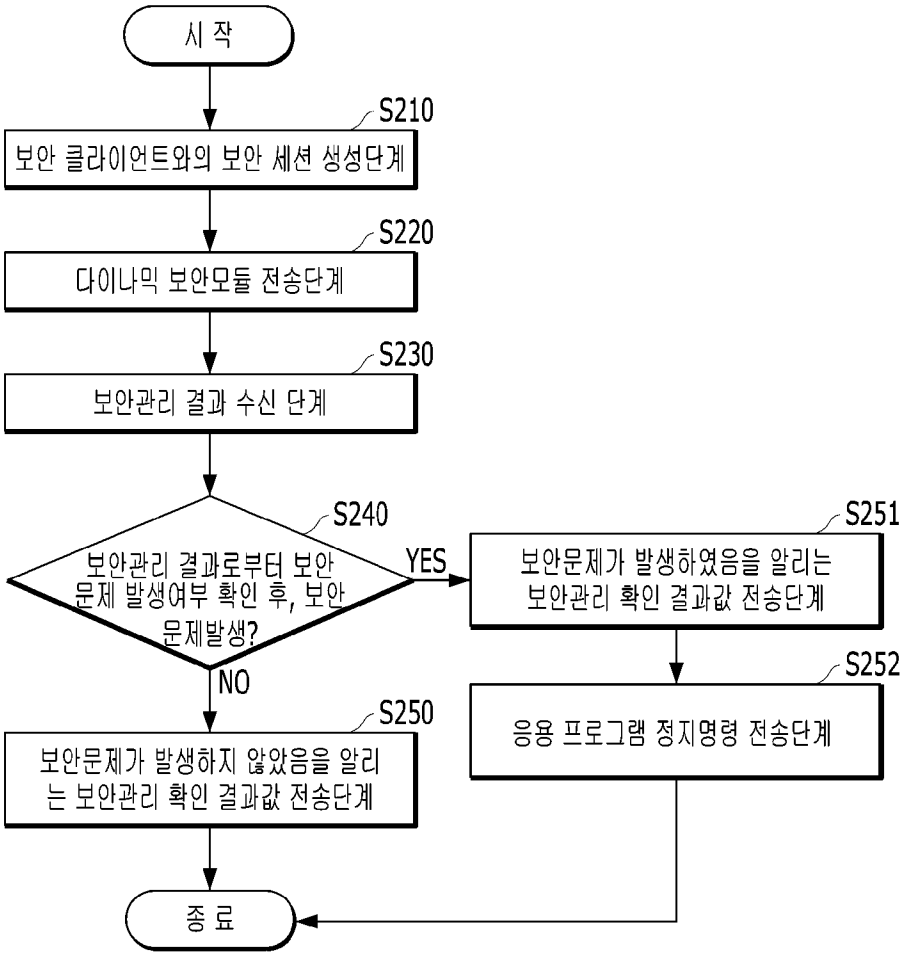
[Fig. 2]



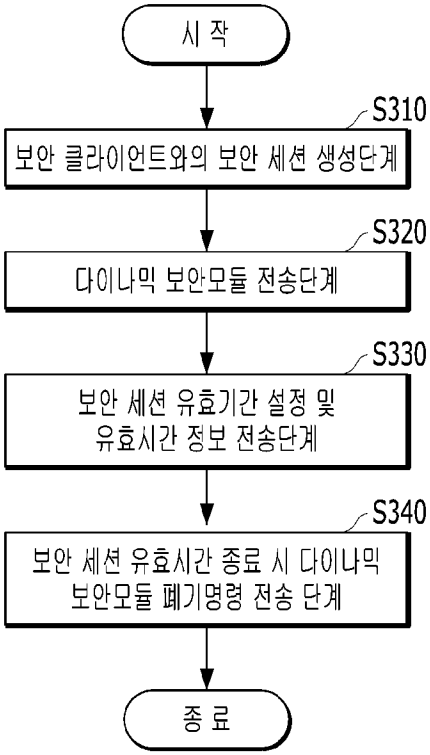
[Fig. 3]

session_id	param1	param2	param3	state1	state2
11836381	A	B	C	1	2
72365784	B	B	A	0	3
87656501	C	A	C	3	2

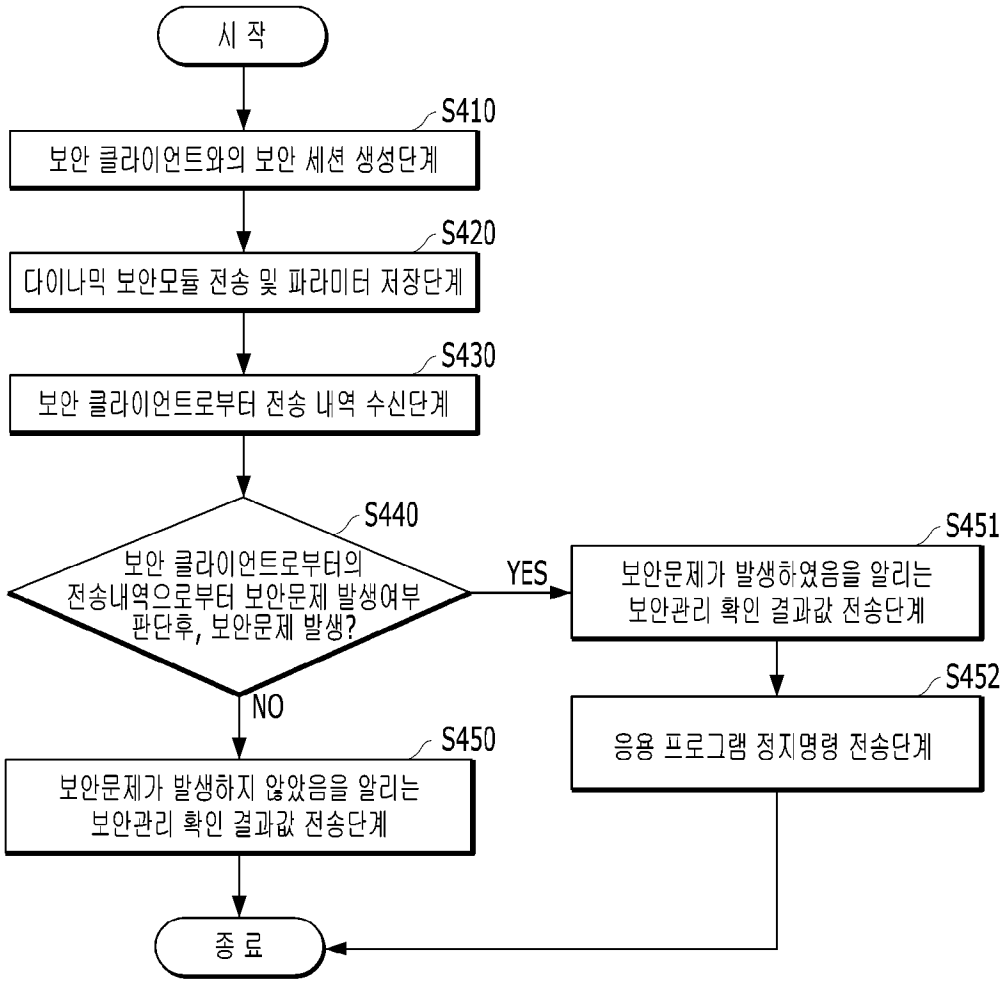
[Fig. 4]


시 작
S210
보안 클라이언트와의 보안 세션 생성단계
S220
다이나믹 보안모듈 전송단계
S230
보안관리 결과 수신 단계
S240
보안관리 결과로부터 보안 문제 발생여부 확인 후, 보안 문제발생?
YES
NO
S251
보안문제가 발생하였음을 알리는 보안관리 확인 결과값 전송단계
S252
응용 프로그램 정지명령 전송단계
S250
보안문제가 발생하지 않았음을 알리는 보안관리 확인 결과값 전송단계
종 료

[Fig. 5]


시 작
S310
보안 클라이언트와의 보안 세션 생성단계
S320
다이나믹 보안모듈 전송단계
S330
보안 세션 유효기간 설정 및 유효시간 정보 전송단계
S340
보안 세션 유효시간 종료 시 다이나믹 보안모듈 폐기명령 전송 단계
종 료

[Fig. 6]


시 작
S410
보안 클라이언트와의 보안 세션 생성단계
S420
다이나믹 보안모듈 전송 및 파라미터 저장단계
S430
보안 클라이언트로부터 전송 내역 수신단계
S440
보안 클라이언트로부터의 전송내역으로부터 보안문제 발생여부 판단후, 보안문제 발생?
YES
NO
S451
보안문제가 발생하였음을 알리는 보안관리 확인 결과값 전송단계
S452
응용 프로그램 정지명령 전송단계
S450
보안문제가 발생하지 않았음을 알리는 보안관리 확인 결과값 전송단계
종 료

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2016/002535

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/51(2013.01)i, G06F 21/50(2013.01)i, G06F 21/52(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/51; G06Q 20/40; H04L 12/26; H04W 12/06; H04W 12/08; H04W 8/24; G06F 21/50; G06F 21/52

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: dynamic security module, service device, user terminal, code, effective time

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2014-0071744 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 12 June 2014 See paragraphs [0027]-[0049]; and figures 2-5.	1-16
Y	KR 10-2014-0023098 A (SK PLANET CO., LTD.) 26 February 2014 See paragraphs [0079]-[0090], [0096]-[0105]; claim 1; and figures 3, 5.	1-16
A	KR 10-2003-0003593 A (HACKERSLAB, CO., LTD.) 10 January 2003 See pages 3-4; and figures 2-4.	1-16
A	KR 10-2014-0127987 A (SK PLANET CO., LTD.) 05 November 2014 See paragraphs [0050]-[0059], [0072]-[0078]; and figures 2, 4.	1-16
A	KR 10-2013-0134946 A (LG CNS CO., LTD.) 10 December 2013 See paragraphs [0055]-[0106]; and figures 2-4.	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 MAY 2016 (31.05.2016)	**01 JUNE 2016 (01.06.2016)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2016/002535

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2014-0071744 A	12/06/2014	NONE	
KR 10-2014-0023098 A	26/02/2014	NONE	
KR 10-2003-0003593 A	10/01/2003	NONE	
KR 10-2014-0127987 A	05/11/2014	NONE	
KR 10-2013-0134946 A	10/12/2013	KR 10-1436202 B1 US 2014-0157353 A1 US 9231914 B2	01/09/2014 05/06/2014 05/01/2016

국 제 조 사 보 고 서

국제출원번호
PCT/KR2016/002535

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/51(2013.01)i, G06F 21/50(2013.01)i, G06F 21/52(2013.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06F 21/51; G06Q 20/40; H04L 12/26; H04W 12/06; H04W 12/08; H04W 8/24; G06F 21/50; G06F 21/52

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 다이나믹 보안모듈, 서버장치, 사용자 단말, 코드, 유효시간

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2014-0071744 A (한국전자통신연구원) 2014.06.12 단락 [0027]-[0049]; 및 도면 2-5 참조.	1-16
Y	KR 10-2014-0023098 A (에스케이플래닛 주식회사) 2014.02.26 단락 [0079]-[0090], [0096]-[0105]; 청구항 1; 및 도면 3, 5 참조.	1-16
A	KR 10-2003-0003593 A ((주) 해커스랩) 2003.01.10 페이지 3-4; 및 도면 2-4 참조.	1-16
A	KR 10-2014-0127987 A (에스케이플래닛 주식회사) 2014.11.05 단락 [0050]-[0059], [0072]-[0078]; 및 도면 2, 4 참조.	1-16
A	KR 10-2013-0134946 A (주식회사 엘지씨엔에스) 2013.12.10 단락 [0055]-[0106]; 및 도면 2-4 참조.	1-16

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2016년 05월 31일 (31.05.2016)	2016년 06월 01일 (01.06.2016)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
진상범
전화번호 +82-42-481-8398

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2016/002535

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2014-0071744 A	2014/06/12	없음	
KR 10-2014-0023098 A	2014/02/26	없음	
KR 10-2003-0003593 A	2003/01/10	없음	
KR 10-2014-0127987 A	2014/11/05	없음	
KR 10-2013-0134946 A	2013/12/10	KR 10-1436202 B1 US 2014-0157353 A1 US 9231914 B2	2014/09/01 2014/06/05 2016/01/05